ROHINI COLLEGE OF ENGINEERING AND TECHNOLOGY
AUTONOMOUS INSTITUTION
Approved by AICTE & Affiliated to Anna University
NBA Accredited for BE (ECE, EEE, MECH) | Accredited by NAAC with A+ Grade
Anjugramam - Kanyakumari Main Road, Palkulam,Variyoor P.O. - 629 401, Kanyakumari District.

Department of Biomedical Engineering

VI Semester

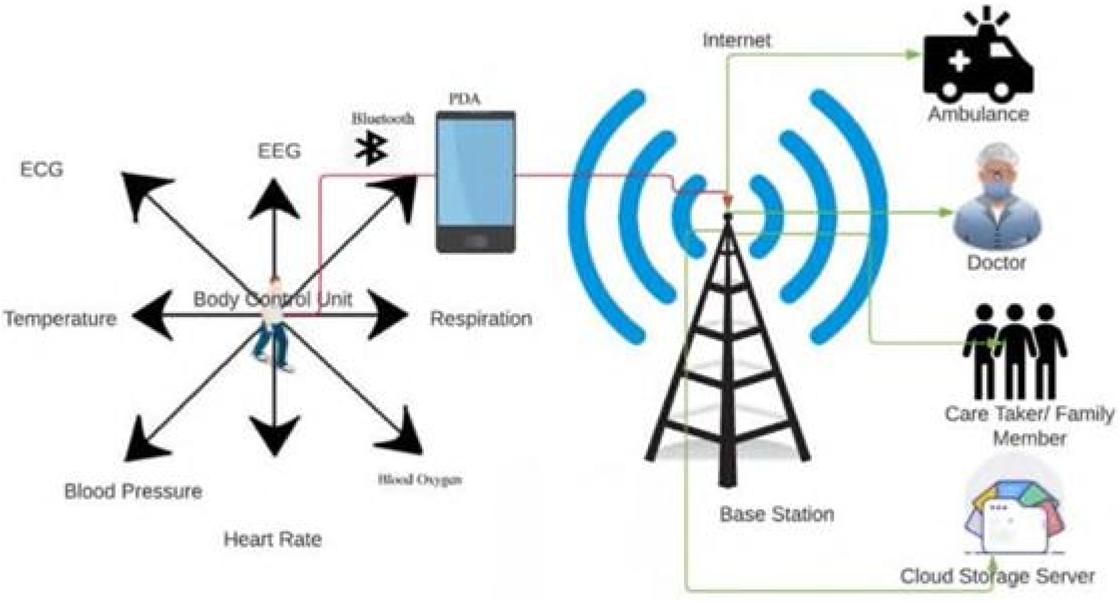
CBM 370 - Wearable Devices

Unit- 3 WIRELESS HEALTH SYSTEMS

3.4 Technical Challenges- System security and reliability

Wireless Health Monitoring System:

Sensor nodes/actuators represent essentially the wireless sensor network, and the sensor node senses acoustic factors including temperature, pressure, sound, pulse rate, ECG, blood pressure, and heart rate of the human body. In healthcare, this form of sensor network is known as a wireless body area network (WBAN)



This diagram represents a wireless health monitoring system. Here's a breakdown of how it works:

1. **Body Control Unit (BCU)**: This collects various physiological signals from the patient, such as:
    - ECG (Electrocardiogram)
    - EEG (Electroencephalogram)
    - Temperature
    - Blood Pressure
    - Heart Rate
    - Respiration
    - Blood Oxygen Levels
2. **Data Transmission**:
    - The BCU sends the collected data to a **PDA (Personal Digital Assistant)** via **Bluetooth**.
    - The PDA then transmits this data wirelessly to a **Base Station** using the Internet.
3. **Cloud and Remote Monitoring**:
    - The base station uploads the data to a **Cloud Storage Server** for secure storage and further analysis.
    - The information is accessible to multiple parties, including:
        - **Doctors** (for medical analysis)
        - **Ambulance services** (for emergency response)
        - **Caregivers or family members** (for continuous monitoring)

Working:

- Wireless body area networks ***consist of*** sensors, biological parameters, body control unit, personal device assistant, transmission factor, and user access.
- Figure shows that the ***wireless body area network*** along with the sensor senses the biological factors continuously in order to obtain the human health information from the body control unit.
- The ***electrocardiogram (ECG) sensor*** records the patient's electric impulse as it passes through the heart muscle. This assists in monitoring the patient's heartbeat, which is used to track various movements such as resting and moving. The temperature of the human body's ears, skin, and forehead are detected by the body temperature sensor.

- ***The pressure of blood*** as it travels through the arteries is measured by blood pressure and the pulse wave is measured by the heart rate sensor as it pumps blood through the patient's body.
- The ***saturation level of oxygen*** in the blood is measured with a pulse oximeter.
- The ***airflow sensor*** can be positioned near the human body's nasal to assess the body's respiration.
- The collected information will be transferred and stored in the ***personal device assistants*** (PDA) and later transmitted to the ***base station***. From the base station, the data will be transferred to the respective ***user applications*** such as cloud databases, ambulances, family members, and doctors via the Internet.
- A ***cloud database's*** purpose is to store the patient's data on a server so that the doctor can access it and then send the patient's information to the user via the internet. Star topology is used in the body area network.
- The body control unit acts as a ***central node*** and then each sensor will sense and communicate to the center node.
- The center node interfaces the human body by using ***Bluetooth or ZigBee*** or Personal Device Assistants (PDA), and then the patient's information can be accessed by the doctors using the Internet.

<u>Security Issues in WBAN:</u>

- The purpose of network security is to protect data from <u>threats</u> during data transmission.
- There are two forms of attacks in network security: <u>active and passive attacks</u>, both of which contribute to the detection of malicious data.
- An <u>active attack</u> is primarily focused on data and has a significant impact on the system's operation.
- A <u>passive attack</u> damages or modifies data but does not degrade information resources.
- The security flaws are applied at various levels. Each layer of the TCP/IP layered architecture generates attacks.
- **IP attacks** are introduced in the second layer (logic link control), resulting in address spoofing for incorrect communication.
- **Internet Control Message Protocol (ICMP) attacks** is generated in the media access control layer, which results in sniffing and man-in-the-middle attacks.

- ❖ In the third network layer, **routing attacks** such as blackhole and eavesdropping attacks are created. TCP attacks are originated in the transport layer, resulting in high synchronization flooding in data communication.
- ❖ **Application layer attacks** are generated in the OSI model's application layer, resulting in authentication issues such as accessing the user's username and password.
- ❖ **A denial of service (DoS) attack** will restrict data from authorized users and prevent them from accessing their resources. Because of the week password, **distributed denial of service (DDoS)** attacks is generated. The main difference between a DOS and a DDOS attack is that a DOS attack targets a single host at a time, but a DDoS attack targets numerous hosts simultaneously.
- ❖ These types of attacks will degrade network performance.
- ❖ The term “reliability” refers to the fact that health-care practitioners receive monitoring data in a timely and accurate manner.
- ❖ WBAN sensors must be capable of viewing and detecting essential active signs of human health; therefore, reliability is critical. WBAN sensors must be capable of viewing and detecting essential active signs of human health; therefore, reliability is critical.

System Security and Reliability Challenges in Wireless Wearable Systems

Wireless wearable health monitoring systems offer significant benefits in remote patient care and real-time health tracking. However, ensuring security and reliability is a major technical challenge. Below are key concerns in these areas:

1. Security Challenges

Wearable systems deal with sensitive personal and medical data, making security a top priority.

a) Data Privacy and Confidentiality

- Wearables collect personal health data that must be protected against unauthorized access.

- Encryption methods (e.g., AES, RSA) must be implemented for secure transmission and storage.
- Compliance with standards like **HIPAA** (Health Insurance Portability and Accountability Act) is crucial.

b) Authentication and Access Control

- Weak authentication mechanisms can lead to unauthorized access.
- Solutions include multi-factor authentication (MFA), biometrics, and blockchain-based access control.

c) Wireless Communication Security

- Wireless transmission (Bluetooth, Wi-Fi, LTE) is prone to eavesdropping and interception.
- Secure protocols like **TLS/SSL**, **VPNs**, and **End-to-End Encryption** can mitigate risks.

d) Malware and Cyberattacks

- Wearable systems can be vulnerable to malware, Denial-of-Service (DoS) attacks, or ransomware.
- Regular security updates, intrusion detection systems (IDS), and anomaly detection help prevent attacks.

2. Reliability Challenges

Ensuring the system remains functional and accurate is crucial for medical applications.

a) Data Accuracy and Integrity

- Sensor drift, noise, or environmental factors can affect the accuracy of measurements.
- Regular calibration and AI-based data validation techniques help maintain accuracy.

b) Continuous Connectivity

- Unstable wireless networks (e.g., weak Bluetooth/Wi-Fi signals) can cause data loss.
- Solutions include multi-network support (LTE/5G backup), edge computing, and data caching.

c) Power Consumption and Battery Life

- Wearables have limited battery life, making energy efficiency critical.
- Low-power communication protocols (BLE, Zigbee) and energy-harvesting techniques (solar, motion-based) help extend battery life.

d) Fault Tolerance and Redundancy

- System failures due to hardware/software issues can endanger patients.
- Redundant data storage, error-checking algorithms, and cloud-based backup solutions improve fault tolerance.

Securing wireless wearable systems requires strong encryption, authentication, and malware protection. Ensuring reliability demands accurate data collection, continuous connectivity, and fault tolerance. Addressing these challenges will enhance trust in wearable healthcare solutions and improve patient safety.

****